

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

## KOREAN PATENT ABSTRACT (KR)

### PUBLICATION

(11) Publication No.: 2000-0012391      (43) Publication Date: 6 March 2000  
(21) Application No.: 1999-0054396      (22) Application Date: 2 December 1998  
(51) IPC Code:  
H04L/58 (Laid-open Earlier)

(71) Applicant:  
Lee, Jae Kyu, International Electronic Commerce Research Center  
F-6, 109-111, Wheki-dong, Dongdaemoon-ku, Seoul, Korea

(72) Inventor:  
SONG, YONG WOOK  
LEE, KAE KYU

(54) Title of the Invention:

Electronic Payment Method and System on the Internet

#### Abstract:

Provided is an electronic payment method for an electronic payment system in which a shopping mall server is connected to a payment server through a leased line. When a client computer purchases goods by accessing the shopping mall server, the shopping mall server issues a transaction number and redirects a web browser of the client computer to be connected to the payment server. Once the client computer is coupled to the payment server, the payment server downloads a log-in window to the client computer, and the client computer transmits a client's ID and password to the payment server. If the transmitted client's ID and password matches those stored in a database of the payment server, the payment server downloads a payment window to the client computer. Then, the client computer transmits payment and transaction information to the payment server, the payment server checks for whether the client can pay for the transaction. If so, the payment server transmits the payment information to the shopping mall server through a leased line. The shopping mall server transmits a transaction confirmation message to the payment server only when the transaction information transmitted from the client computer matches the transaction information stored in its own database. When the payment server receives the transaction confirmation message from the shopping mall server through the leased line, it performs payment by account-to-account fund transfer or a credit card based on the transaction information and payment information.

(19) 대한민국특허청(KR)

(12) 공개특허공보(A)

(51) Int. Cl.<sup>5</sup>

H04L 12/58(조기공개)

(11) 공개번호 특2000-0012391

(43) 공개일자 2000년 03월 06일

(21) 출원번호 10-1999-0054396

(22) 출원일자 1999년 12월 02일

(71) 출원인 (사) 국제전자상거래 연구센터 이재규

(72) 발명자 서울특별시 동대문구 회기동 109-111 에프 -6

송용욱

경상남도 진주시 신안동 평거2차 현대아파트 202-903호

이재규

서울특별시 동대문구 회기동 109-111 에프 -6

(74) 대리인 김삼수

상사청구 : 있음

(54) 인터넷 상에서의 전자결제방법 및 시스템

요약

쇼핑몰서버와 결제서버의 사이가 전용선으로 연결되어 있는 전자결제시스템에서의 전자결제방법에 제공된다. 고객 컴퓨터에서 쇼핑몰서버에 접속하여 물품을 구입하면 쇼핑몰서버에서는 거래번호를 생성하고 고객컴퓨터의 웹브라우저가 결제서버에 자동적으로 연결되도록 리다이렉트시킨다. 리다이렉트에 의해 고객 컴퓨터가 결제서버에 연결되면 결제서버에서 로그인 화면을 보내고, 고객 컴퓨터에서는 고객의 ID와 패스워드를 결제서버로 전송하며, ID와 패스워드가 결제서버의 데이터베이스에 저장되어 있는 ID 및 패스워드와 일치하는 경우에 결제서버에서 고객 컴퓨터로 지불화면을 보냄에 따라, 고객 컴퓨터에서 결제서버에 지불정보와 거래정보를 전송하고, 결제서버에서는 해당 고객이 결제가 가능한지를 확인하며, 결제가 가능한 경우에만 상기 전용선을 통해 쇼핑몰 서버에 거래정보를 전송한다. 쇼핑몰서버는 쇼핑몰서버에서 저장되어 있는 거래정보가 고객 컴퓨터에서 전송된 거래정보와 일치하는지 확인하며, 일치되는 경우에만 거래확인 메시지를 결제서버에 전송한다. 결제서버는 거래확인 메시지가 전용선을 통해 쇼핑몰서버로부터 수신되면 거래정보 및 지불정보에 따라 계좌이체나 신용카드지불승인 등의 결제처리를 수행한다.

도표

도3

색인어

전자상거래, 전자결제, 인증, 보안, 암호화, 전자서명

## **명세서**

### **도면의 간단한 설명**

도 1은 본 발명의 구성요소들이 인터넷망과 전용망을 통해 연결되어 있는 모습을 보여주는 개략도이다.

도 2는 본 발명의 결제방법에서의 절차에 따른 정보의 흐름을 보여주는 개략도이다.

도 3은 본 발명의 결제방법에서의 각 구성요소의 동작과 그에 따른 데이터의 흐름을 보여주는 데이터 흐름도이다.

도 4는 본 발명의 결제방법에서 지불취소에 따른 각 구성요소의 동작과 그에 따른 데이터의 흐름을 보여주는 데이터 흐름도이다.

도 5는 본 발명의 결제방법에서 결제가 불가능한 경우, 또는 거래가 불가능한 경우의 각 구성요소의 동작과 그에 따른 데이터의 흐름을 보여주는 데이터 흐름도이다.

도 6은 고객이 인터넷 쇼핑몰에서 상품을 구매신청을 하기 위한 주문화면의 예이다.

도 7은 고객이 결제서버에 결제를 하기 위한 지불화면의 예이다.

### **발명의 상세한 설명**

#### **발명의 목적**

#### **발명이 속하는 기술 및 그 분야의 종래기술**

본 발명은 인터넷상에서의 전자지불방법 및 시스템에 관한 것으로서, 더욱 상세하게는 인터넷상에서의 거래에 따른 지불을 안전하게 행할 수 있는 전자지불방법 및 시스템에 관한 것이다.

인터넷의 발달에 따라 인터넷을 통한 상거래가 급속히 증가하고 있다. 상거래에는 필연적으로 대금의 지불이 수반되게 된다. 전자상거래에서도 이는 예외가 아니다.

상거래에 있어서, 구매장소와 대금지불 장소가 달라지는 것은 별로 바람직하지 않다. 예를 들면, 물건의 구매는 인터넷상에서 하고 대금지불은 구매자로 하여금 직접 은행에 가서 송금하게 하거나, 전화 혹은 우편으로 신용카드번호를 알려주는 방식을 채택하게 되면, 구매자나 판매자 모두 불편하기 때문이다. 결국, 인터넷상에서도 현실세계에서와 마찬가지로 물건의 구매와 함께 바로 대금지불이 이루어질 수 있어야 한다.

이러한 점 때문에 다양한 전자지불시스템이 제안되거나 사용되고 있다. 이러한 예로는 신용카드를 이용한 지불 시스템, 전자 자금이체, 전자수표 시스템, IC 카드형 전자현금 시스템 등을 들 수 있다.

그중에서, 인터넷 신용카드 지불 시스템은 인터넷을 통해 신용카드 번호를 상인에게 전달하여 상거래가 이루어지도록 하는 지불 시스템이다. 신용카드를 사용한 지불은 기존의 실세계에서 신용카드로 지불을 하는 것과 거의 같은 절차로 이루어지고, 기존의 신용카드 결제망을 사용하므로 구현이 쉽다. 따라서 인터넷상에서 가장 많이 사용되고 있는 지불방식이다

그러나, 신용카드를 이용한 지불에서 네트워크를 통해 전달되는 정보에는 사용자의 신상에 관한 정보와 신용카드에 관한 정보가 포함된다. 따라서, 해킹으로부터의 보안이 중요하다.

이러한 점을 해결하기 위해서, 미국특허 제5,778,173호에서는 고객과 지불시스템과의 사이를 인터넷이 아닌 별도의 회선으로 접속하여 이러한 정보를 전송하도록 하고 있다. 그러나, 고객은 인터넷 쇼핑몰에서 물건을 구입할 때 지불을 하기 위해서는 지불시스템에 별도의 회선으로 접속해야 하므로 매우 불편하다는 단점이 있다.

신카드를 이용한 지불시스템에 있어서 또 한가지 중요한 점은, 상인이 고객의 신용카드 번호를 모르게 해야 한다는 점이다. 만약 상인이 고객의 신용카드 번호를 알 수 있다면, 고객 몰래 상인이 신용카드 번호를 이용해 불법적인 거래를 발생시킬 수 있는 가능성이 남아 있는 것이다.

현재, 많은 인터넷 쇼핑몰에서는 신용카드번호를 쇼핑몰에 전송하도록 되어 있기 때문에 이러한 문제점이 상존하고 있다. 이러한 점 때문에, 미국특허 제5,778,173호에서는 신용카드정보를 고객이 직접 별도의 회선으로 지불시스템에 전송하면, 지불시스템에서는 결제가 가능하다는 사실을 쇼핑몰에 알려주도록 함으로써 신용카드번호가 상인에게 전달되지 않도록 하고 있지만, 위에서 설명한 것처럼 지불을 하기 위해서 고객이 별도의 회선으로 지불시스템에 연결해야 한다는 문제점이 있다.

또한, 고객이 발생한 거래에 대해 부인할 수 없도록 해야 한다는 점도 중요하다. 악의의 카드 소지자가 인터넷을 통해 물건을 구입해놓고는, 그런 사실이 없다고 부인하는 것을 방지할 수 있어야 한다.

#### **발명이 이루고자 하는 기술적 과제**

#### **발명의 구성 및 작용**

#### **발명의 효과**

#### **발명이 이루고자 하는 기술적 과제**

본 발명은 이러한 점을 감안하여 이루어진 것으로서, 인터넷상에서 물건의 구매와 함께 바로 결제처리가 이루어지도록 할 수 있는 전자결제방법 및 시스템을 제공하는 것을 목적으로 한다.

본 발명의 다른 목적은 사용자의 신상에 관한 정보와 은행계좌나 신용카드와 같은 결제수단에 관한 정보에 대한 해킹의 염려가 적은 전자결제방법 및 시스템을 제공하는 것이다.

본 발명의 다른 목적은 사용자의 계좌번호나 신용카드번호를 쇼핑몰에 알리지 않고도 결제할 수 있는 전자결제방법 및 시스템을 제공하는 것이다.

본 발명의 다른 목적은 사용자가 자신의 구입 사실을 부인하는 것을 방지할 수 있는 전자결제방법 및 시스템을 제공하는 것이다.

### **발명의 구성 및 작용**

이하, 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명한다.

도 1은 본 발명의 구성요소들이 인터넷망과 전용망을 통해 연결되어 있는 모습을 보여주는 개략도이다.

인터넷 사용자(100)는 인터넷망(200)을 통해 쇼핑몰서버(300)에 접속한다. 인터넷망(200)에는 또한 결제서버(400)가 연결되어 있어서, 인터넷 사용자(100)가 결제서버(400)를 통해 결제를 할 수 있도록 되어 있다. 쇼핑몰서버(300)와 결제서버(400)는 서로 전용선 또는 별도의 암호 프로토콜에 따른 가상전용선(VPN)(500)을 통해 연결되어 있다. 전용선을 사용하는 경우에도 암호화를 병행하는 것은 물론 가능하다.

도 2를 참조하여 본 발명의 결제방법을 개략적으로 설명한다. 도 2는 본 발명의 결제방법에서의 절차에 따른 정보의 흐름을 보여주는 개략도이다.

먼저, 고객(100)이 쇼핑몰서버(300)에 접속하여 상품을 주문하면 주문정보가 인터넷망을 통해 쇼핑몰서버(300)에 전달된다(도 2의 ①). 그러면, 쇼핑몰서버(300)는 결제서버(400)의 URL을 고객(100)의 웹브라우저로 보낸다(도 2의 ②). 이때, 결제서버(400)의 URL에는 거래번호와 금액이 포함된다.

고객(100)의 웹브라우저는 쇼핑몰서버(300)로부터의 URL에 따라 자동적으로 결제서버(400)에 접속하게 된다(도 2의 ③). 결제서버(400)에 접속하면 지불정보와 거래번호, 금액이 결제서버(400)에 전달되게 된다.

고객(100)이 결제서버(400)에 접속하면, 결제서버(400)는 전용선 또는 가상전용선(500)을 통해 거래번호와 금액을 쇼핑몰서버(300)에 보낸다(도 2의 ④). 그러면, 쇼핑몰서버(300)는 해당 내용이 맞는지를 확인하여 마찬가지로 전용선 또는 가상전용선(500)을 통해 그 결과를 결제서버에게 전송한다(도 2의 ⑤).

쇼핑몰서버(300)로부터 거래확인을 받으면, 결제서버(400)는 지불확인 화면을 고객(100)의 웹브라우저에 보냄으로써, 고객의 상품구매에서 지불까지의 절차가 종료되게 된다.

다음으로 도 3 내지 도 5를 사용하여 본 발명의 바람직한 실시예에 따른 결제방법을 상세히 설명한다.

도 3은 본 발명의 결제방법에서의 각 구성요소의 동작과 그에 따른 데이터의 흐름을 보여주는 데이터 흐름도이며, 도 4는 본 발명의 결제방법에서 지불취소에 따른 각 구성요소의 동작과 그에 따른 데이터의 흐름을 보여주는 데이터 흐름도이며, 도 5는 본 발명의 결제방법에서 결제가 불가능한 경우, 또는 거래가 불가능한 경우의 각 구성요소의 동작과 그에 따른 데이터의 흐름을 보여주는 데이터 흐름도이다.

먼저, 고객(100)이 쇼핑몰서버(300)에 접속하여 상품을 선택한 다음 구입버튼을 누른다. 그러면 도 6에 도시된 것과 같은 화면이 나타난다. 고객은 여러가지 지불방법 중에서 본 발명에 따른 결제방법을 선택한다. 도 6에서는 편의상 본 발명에 따른 결제방법의 명칭을 "한빛전자지불"이라고 명명하였다. 이때, 고객은 결제서버(400)의 운영기관(은행, 신용카드사 등의 금융기관)에 계좌를 가지고 있어야 한다. 이 계좌는 은행계좌일 수도 있고, 신용카드일 수도 있으며, 또는 별도의 전자지불용 계좌일 수도 있다.

그러면, 구입상품명, 수량, 가격 등의 주문정보가 쇼핑몰서버(300)에 전송된다(10). 쇼핑몰서버(300)는 주문정보를 받으면 거래번호를 생성한다. 또한, 쇼핑몰서버(300)는 결제를 위하여 고객(100)의 웹브라우저를 결제서버(400)로 리다이렉트

(redirect)하도록 한다(12).

이렇게 리다이렉트 시키는 방법으로는 HTTP의 "Location" 헤더를 사용하면 된다. 즉, 예를 들어 C로 된 CGI 프로그램의 경우에 다음과 같은 구문을 사용하면 된다:

```
printf("Location: http://www.hanvit.com/cgi-bin/login.cgi?TID=123&AMOUNT=220000\n\n");
```

그러면, 결제서버(400)의 로그인 프로그램에 거래번호(TID) 123과 금액(AMOUNT) 22만원이 전달된다(14).

상기 리다이렉션에 의해 고객(100)이 결제서버(400)에 접속하게 되면, 결제서버(400)는 고객(100)에게 로그인 화면을 내 보낸다. 또한, 결제서버(400)는 결제서버에서 보내온 정당한 화면임을 나타내기 위해서 결제서버의 인증서도 함께 전송한다(16). 리다이렉션에 의해 전송된 거래번호(TID)와 금액(AMOUNT)은 히든 필드(hidden field)로 처리되어 다음 화면으로 넘어가게 된다.

결제서버(400)로부터 결제서버 로그인 화면과 결제서버 인증서를 받은 고객(100)의 컴퓨터는 그 컴퓨터에 설치되어 있는 본 발명에 따른 결제용 프로그램을 사용하여 인증서를 확인하여 정당한 결제서버로부터의 로그인 화면인지를 확인한다.

정당한 결제서버로부터의 로그인 화면인지가 확인되면 결제용 프로그램은 세션키(SK)를 생성시키고, 세션키(SK)를 결제서버의 공개키(PBkb)로 암호화한다. 또한, 고객(100)이 입력한 ID와 패스워드를 세션키(SK)로 암호화한다. 암호화된 세션키(PBkb(SK))와 암호화된 ID 및 패스워드(SK(ID,passwd))는 결제서버(400)로 전송되게 된다(18).

암호화된 세션키와 ID, 패스워드를 수신한 결제서버(400)는 자신의 개인키(PVKb)로 암호화된 세션키(PBkb(SK))의 암호를 풀어서 세션키(SK)를 복구한다. 그리고, 복구된 세션키(SK)로 암호화된 ID 및 패스워드(SK(ID,passwd))의 암호를 풀어서 ID와 패스워드를 복구한다.

결제서버(400)는 복구된 ID 및 패스워드와, 결제서버(400)의 데이터베이스에 저장되어 있는 ID 및 패스워드를 비교한다. 비교한 결과, 고객(100)이 입력한 ID와 패스워드가 일치하면 결제서버(400)는 도 7과 같은 지불화면을 고객(100)의 웹브라우저로 출력한다(20).

고객(100)은 도 7과 같은 지불화면에서 자신의 계좌번호와 계좌의 비밀번호 등과 같은 지불정보를 입력한다.

이때, 결제서버(400)는 고객(100)의 ID로부터 그 고객(100)의 계좌번호를 알 수 있으므로, 지불화면을 보낼 때 계좌번호가 미리 입력되어 있는 상태로 보내서 고객(100)이 일일이 자신의 계좌번호를 입력하지 않아도 되도록 하는 것도 물론 가능하다.

고객(100)이 도 7의 화면에서 지불정보를 입력하고 확인 버튼을 클릭하면, 고객(100)의 컴퓨터에 설치되어 있는 결제용 프로그램은 다시 지불정보(PI), 거래번호(TID), 금액(AMOUNT)을 세션키(SK)로 암호화한다. 암호화된 지불정보, 거래번호, 금액(SK(PI, TID, AMOUNT))은 결제서버(400)로 전송된다(22).

암호화된 지불정보를 수신한 결제서버(400)는 세션키(SK)로 이 메시지의 암호를 풀어서 지불정보, 거래번호, 금액을 복구시킨 다음, 저장해둔다.

결제서버(400)는 이 정보로부터 해당 고객(100)이 해당 금액을 결제할 수 있는지를 확인한다. 즉, 해당 고객의 계좌에 해당 금액을 결제할 수 있는 잔고가 있는지 또는 해당 고객이 거래정지된 것은 아닌지와 같은 결제 가능여부를 확인한다.

확인 결과, 결제가 가능하지 않은 경우에는 도 5의 (a)에 도시한 것처럼 지불이 불가능함을 나타내는 지불불가 화면을 고객(100)에게 전송한다(50). 지불불가화면은 예를 들면, "잔고가 부족하여 결제를 할 수 없습니다"라든가 "거래가 정지되어 있는 계좌입니다"와 같은 메시지를 포함할 수 있다.

확인 결과, 결제가 가능하다고 판단되면, 결제서버(400)는 거래번호(TID), 금액(AMOUNT)에 대한 전자서명(OS(TID,

AMOUNT)을 생성한다. 그리고, 전용선 또는 가상전용선(500)을 통해 쇼핑물서버(300)에 거래번호(TID), 금액(AMOUNT) 및 전자서명(OS(TID, AMOUNT))을 전달한다.

쇼핑물서버(300)와 결제서버(400) 사이에서는 TCP/IP 소켓 프로그램에 의한 클라이언트/서버 구조에 의해 통신하는 것이 바람직하다. 여기에서, 결제서버(400)는 클라이언트 역할을 하고 쇼핑물서버(300)는 서버 역할을 한다.

전자서명을 덧붙이는 이유는 인증(Authentication)과 무결성(Integrity)을 확보하기 위함이다. 또한 결제서버(400)는 결제서버 인증서도 함께 전송한다(24).

이 메시지를 수신한 쇼핑물서버(300)는 결제서버 인증서와 전자서명을 확인한다. 그리고, 수신된 거래번호와 금액을 자신이 가지고 있는 거래정보와 비교한다. 두 데이터가 서로 일치하면, 거래확인에 대한 전자서명(OS(거래확인))을 생성하고, 쇼핑물 인증서와 함께 전용선 또는 가상전용선(500)을 통해 결제서버(400)로 전송한다(26).

거래를 확인한 후, 쇼핑물서버(300)는 고객(100)이 주문한 상품을 고객(100)에게 배달한다(30). 상품의 배달방법은 가능한 어떠한 방법을 채택해도 상관없으며, 본 발명은 특정 배달방법에 한정되는 것은 아니다. 또한, 구입한 상품이 MP3 파일과 같은 디지털 콘텐츠인 경우에는 온라인으로 다운로드하는 것도 물론 가능하다.

결제서버(400)로부터의 거래정보와 자신이 갖고 있는 거래정보가 일치하지 않은 경우에는, 쇼핑물서버(300)는 도 5의 (b)에 도시한 것처럼 거래불가에 대한 전자서명을 생성한 후, 쇼핑물 인증서와 함께 결제서버(400)에 전송한다(60).

쇼핑물서버(300)로부터 메시지를 수신한 결제서버(400)는 인증서와 전자서명을 확인한다.

수신된 메시지가 거래를 확인하는 메시지인 경우에는 해당 금액을 고객(100)의 계좌에서 쇼핑물의 계좌로 이체(또는, 신용카드의 경우에는 지불승인)시킨다. 그리고, 지불이 이루어졌음을 나타내는 지불확인화면을 고객(100)의 컴퓨터로 보낸다(28). 지불확인화면은 예를 들면 "지불이 완료되었습니다" 또는 "홍길동님의 계좌에서 0000원이 인출되었습니다"와 같은 메시지를 포함한다. 이상의 절차에 의해서 본 발명에 따른 정상적인 결제는 종료되게 된다.

수신된 메시지가 거래불가 메시지인 경우에는 도 5의 (b)에 도시된 것처럼 거래가 불가능함으로 나타내는 거래불가화면을 고객(100)의 컴퓨터로 보낸다(62). 거래불가화면은 예를 들면 "거래정보가 일치되지 않아서 지불이 되지 않았습니다. 다시 한번 구매신청을 하시거나 해당 쇼핑물에 문의하시기 바랍니다"와 같은 메시지를 포함한다.

다음으로, 결제를 하고 난 고객이 지불을 취소하고자 하는 경우의 절차에 대해서 도 4를 참조하여 설명한다.

지불취소는 온라인 상으로 이루어지는 것이 아니라, 고객(100)이 쇼핑물 담당자에게 전화나 기타 통신수단을 사용하여 요청함으로써 이루어진다.

고객으로부터 지불을 취소할 것을 요청받은 쇼핑물서버(300)는 지불취소에 대한 전자서명을 생성하여 지불취소 및 지불취소에 대한 전자서명(OS(지불취소))을 쇼핑물 인증서와 함께 전용선 또는 가상전용선(500)을 통해 결제서버(400)로 전송한다(40).

쇼핑물서버(300)와 결제서버(400) 사이에서는 TCP/IP 소켓 프로그램에 의한 클라이언트/서버 구조에 의해 통신하는 것이 바람직하다. 여기에서, 결제서버(400)는 서버 역할을 하고 쇼핑물서버(300)는 클라이언트 역할을 한다.

쇼핑물서버(300)로부터 지불 취소 메시지를 수신한 결제서버(400)는 인증서와 전자서명을 확인하고, 정당한 메시지인 경우에는 지불을 취소하는 역계좌이체를 수행한다. 즉, 지불금액을 쇼핑물의 계좌에서 고객의 계좌로 이체(신용카드의 경우 승인취소 또는 역거래 발생)한다.

그리고, 취소확인에 대한 전자서명을 생성하여 취소확인 및 취소확인에 대한 전자서명(OS(취소확인))을 결제서버 인증서와 함께 전용선 또는 가상전용선(500)을 통해 쇼핑물서버(300)로 전송한다(42).



결제서버(400)로부터 취소확인을 받은 쇼핑몰은 해당 거래내역을 삭제하고, 고객으로부터 배달 상품을 회수함으로써 지불 취소절차가 완료하게 된다.

다음으로 각 구성요소 간의 보안방법에 대해서 설명한다.

### 1. 고객(100)과 쇼핑몰(300) 사이

쇼핑몰에서의 고객의 인증은 그다지 중요하지 않으므로 간단하게 사용자 ID와 비밀번호를 사용하여 인증하도록 할 수 있다. 물론, 다른 복잡한 방법을 사용하는 것도 가능하다.

쇼핑몰의 인증은 SSL(Secured Socket Layer)의 인증서를 사용할 수 있을 것이다. 물론, 다른 인증방법을 사용하는 것도 가능하다.

또한, 네트워크의 보안, 즉 기밀성(confidentiality)과 무결성(integrity)도 이 단계에서는 그다지 중요하지 않으므로 SSL과 같은 간단한 보안을 사용하는 것이 가능하지만, 이에 한정되는 것은 아니다.

### 2. 고객(100)과 결제서버(400) 사이

고객(100)과 결제서버(400) 사이의 보안문제는 고객(100)과 쇼핑몰(300) 사이의 보안문제에 비해서 다소 중요하다.

따라서, 고객인증은 계좌번호와 그 비밀번호, 결제서버(400)에의 고객의 ID와 그 패스워드를 사용한다. 또한, 세션키에 의한 일회성 패스워드(one-time password)를 사용할 수도 있다.

결제서버(400)의 인증은 SSL(Secured Socket Layer)의 인증서를 사용할 수 있을 것이다. 물론, 다른 인증방법을 사용하는 것도 가능하다.

또한, 네트워크의 보안, 즉 기밀성(confidentiality)과 무결성(integrity)도 SSL을 사용할 수 있지만, 이에 한정되는 것은 아니다.

### 3. 쇼핑몰서버(300)와 결제서버(400) 사이

쇼핑몰서버(300)와 결제서버(400)의 인증은 별도의 전용선을 사용하여 보안이 이루어진다. 또한, 별도의 전용선을 사용하면서도 암호화를 병행함으로써 보안등급을 높일 수도 있다.

별도의 전용선을 사용하는 대신 별도의 암호 프로토콜(전자서명)에 따른 가상전용선(VPN)을 사용하는 것도 가능하다.

네트워크의 보안도 별도의 전용선(암호화 병행 가능)을 사용하거나 또는 별도의 암호 프로토콜에 따른 가상전용선을 사용함으로써 이루어진다.

이상 본 발명을 상세히 설명하였지만, 본 발명은 특정 실시예에 한정되는 것은 아니다. 본 발명이 속하는 기술분야에서 통상의 지식을 지닌 자라면 본 발명의 사상에서 벗어나지 않으면서 많은 변형과 수정을 가할 수 있음을 이해할 것이다.

## **발명의 효과**

본 발명에 따르면, 고객이 인터넷 쇼핑몰에서 대금지불을 선택하면 자동적으로 인터넷을 통해 결제서버에 접속되어 결제 행위가 이루어지므로, 인터넷상에서 물건의 구매와 함께 바로 대금지불이 이루어질 수 있게 되어 결제가 편리해진다는 효과가 있다.

또한, 사용자의 신상에 관한 정보와 신용카드나 계좌번호와 같은 결제수단에 관한 정보가 암호화되어 전송되므로 해킹의 염려가 적다는 효과가 있다.

또한, 지불정보는 고객과 결제서버 사이에서만 수수되므로 쇼핑몰에서는 지불정보를 알 수 없게 되어, 지불정보의 유출에 따른 문제점을 해결할 수 있다는 효과가 있다.

또한, 고객과 결제서버 사이에서는 전자서명에 의해 인증이 되고, 결제서버와 쇼핑몰 서버 사이에서는 별도의 전용선에 의해 또는 전자서명에 의해 인증이 되므로 각 결제주체 사이에서 자신의 행위를 부정할 수 없게 되어, 신뢰성 있는 거래를 행할 수 있다는 효과가 있다.

## **(57) 청구의 범위**

**청구항 1.** 인터넷 망에 연결된 고객 컴퓨터와,

인터넷 망에 연결된 쇼핑몰서버와,

인터넷 망에 연결된 결제서버를 구비하되,

상기 쇼핑몰서버와 상기 결제서버의 사이는 전용선으로 연결되어 있으며,

상기 고객 컴퓨터에서 상기 쇼핑몰서버에 접속하여 물품을 구입하면 상기 쇼핑몰서버에서는 거래번호를 생성하고 상기 고객컴퓨터의 웹브라우저가 상기 결제서버에 자동적으로 연결되도록 리다이렉트시키며,

상기 리다이렉트에 의해 고객 컴퓨터가 상기 결제서버에 연결되면 상기 결제서버에서 로그인 화면을 보내고, 상기 고객 컴퓨터에서는 고객의 ID와 패스워드를 상기 결제서버로 전송하며,

상기 고객의 ID와 상기 패스워드가 상기 결제서버의 데이터베이스에 저장되어 있는 ID 및 패스워드와 일치하는 경우에 상기 결제서버에서 상기 고객 컴퓨터로 지불화면을 보냄에 따라, 상기 고객 컴퓨터에서 상기 결제서버에 계좌비밀번호 또는 신용카드번호를 포함하는 지불정보와 금액 및 상기 생성된 거래번호를 포함하는 거래정보를 전송하고, 상기 결제서버에서는 해당 고객이 결제가 가능한지를 확인하여, 결제가 가능한 경우에만 상기 전용선을 통해 상기 쇼핑몰 서버에 거래정보를 전송하며,

상기 쇼핑몰서버는 상기 거래정보를 수신하면, 상기 쇼핑몰서버에서 저장되어 있는 거래정보가 고객 컴퓨터에서 전송된 거래정보와 일치하는지 확인하여, 일치되는 경우에만 거래확인 메시지를 상기 결제서버에 전송하며,

상기 결제서버는 거래확인 메시지가 상기 전용선을 통해 상기 쇼핑몰서버로부터 수신되면 상기 거래정보 및 지불정보에 따라 지불을 수행하는 것을 특징으로 하는 인터넷 상에서의 전자결제시스템.

**청구항 2.** 제1항에 있어서, 상기 전용선은 암호 프로토콜에 의한 가상전용선인 것을 특징으로 하는 인터넷 상에서의 전자결제시스템.

**청구항 3.** 제1항에 있어서, 상기 전용선은 물리적으로 분리된 전용선인 것을 특징으로 하는 인터넷 상에서의 전자결

제시스템.

**청구항 4.** 제1항 내지 제3항중 어느 한 항에 있어서,

상기 고객컴퓨터는 상기 결제서버로 상기 ID 및 패스워드를 전송할 때 세션키를 생성하여 상기 세션키로 상기 ID 및 패스워드를 암호화해서 전송하며,

상기 고객컴퓨터에서 상기 결제서버로 지불정보 및 거래정보를 전송할 때, 이들 정보를 상기 세션키로 암호화하여 전송하는 것을 특징으로 하는 인터넷 상에서의 전자결제시스템.

**청구항 5.** 제1항 내지 제3항중 어느 한 항에 있어서,

상기 쇼핑몰 서버는 상기 고객이 구매를 취소하면 지불취소에 대한 전자서명을 생성하여 결제서버에 전송하며,

상기 결제서버는 지불취소에 대한 상기 전자서명을 확인하여 정당한 전자서명인 경우에는 지불을 취소하고 취소확인에 대한 전자서명을 생성하여 상기 쇼핑몰서버에 전송하는 것을 특징으로 하는 인터넷 상에서의 전자결제방법.

**청구항 6.** 인터넷 망에 각각 연결되어 있는 고객 컴퓨터, 쇼핑몰서버, 결제서버를 구비하되, 상기 쇼핑몰서버와 상기 결제서버의 사이는 전용선으로 연결되어 있는 전자결제시스템을 사용한 전자결제방법에 있어서,

상기 고객 컴퓨터에서 상기 쇼핑몰서버에 접속하여 물품을 구입하면 상기 쇼핑몰서버에서는 거래번호를 생성하고 상기 고객컴퓨터의 웹브라우저가 상기 결제서버에 자동적으로 연결되도록 리다이렉트시키는 제1단계와,

상기 리다이렉트에 의해 고객 컴퓨터가 상기 결제서버에 연결되면 상기 결제서버에서 로그인 화면을 보내고, 상기 고객 컴퓨터에서는 고객의 ID와 패스워드를 상기 결제서버로 전송하는 제2단계와,

상기 고객의 ID와 상기 패스워드가 상기 결제서버의 데이터베이스에 저장되어 있는 ID 및 패스워드와 일치하는 경우에 상기 결제서버에서 상기 고객 컴퓨터로 지불화면을 보냄에 따라, 상기 고객 컴퓨터에서 상기 결제서버에 계좌비밀번호 또는 신용카드번호를 포함하는 지불정보와 금액 및 상기 생성된 거래번호를 포함하는 거래정보를 전송하고, 상기 결제서버에서는 해당 고객이 결제가 가능한지를 확인하여, 결제가 가능한 경우에만 상기 전용선을 통해 상기 쇼핑몰 서버에 거래정보를 전송하는 제3단계와,

상기 쇼핑몰서버는 상기 거래정보를 수신하면, 상기 쇼핑몰서버에서 저장되어 있는 거래정보가 고객 컴퓨터에서 전송된 거래정보와 일치하는지 확인하여, 일치되는 경우에만 거래확인 메시지를 상기 결제서버에 전송하는 제4단계와,

상기 결제서버는 거래확인 메시지가 상기 전용선을 통해 상기 쇼핑몰서버로부터 수신되면 상기 거래정보 및 지불정보에 따라 지불을 수행하는 제5단계

를 구비하는 것을 특징으로 하는 인터넷 상에서의 전자결제방법.

**청구항 7.** 제6항에 있어서, 상기 전용선은 암호 프로토콜에 의한 가상전용선인 것을 특징으로 하는 인터넷 상에서의 전자결제방법.

**청구항 8.** 제6항에 있어서, 상기 전용선은 물리적으로 분리된 전용선인 것을 특징으로 하는 인터넷 상에서의 전자결제방법.

**청구항 9.** 제6항 내지 제8항중 어느 한 항에 있어서,

상기 제2단계에서 상기 고객컴퓨터는 상기 결제서버로 상기 ID 및 패스워드를 전송할 때 세션키를 생성하여 상기 세션키로 상기 ID 및 패스워드를 암호화해서 전송하며,

상기 제3단계에서 상기 고객컴퓨터는 상기 결제서버로 지불정보 및 거래정보를 전송할 때, 이들 정보를 상기 세션키로 암호화하여 전송하는 것을 특징으로 하는 인터넷 상에서의 전자결제방법.

**청구항 10.** 제6항 내지 제8항중 어느 한 항에 있어서,

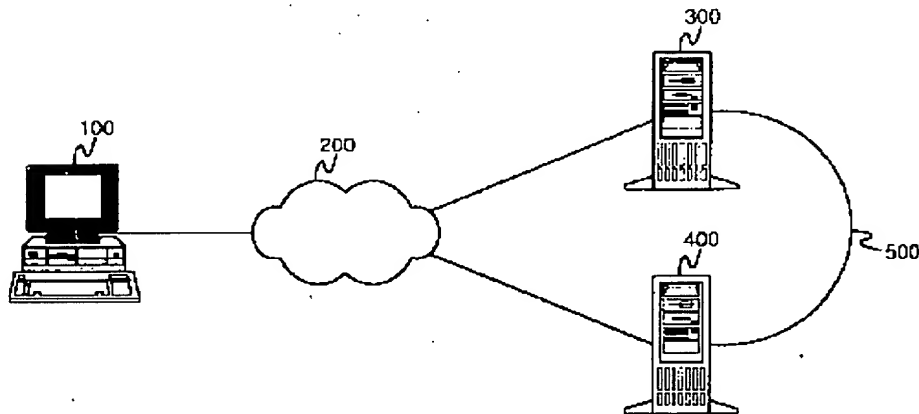
상기 고객이 구매를 취소함에 따라 상기 쇼핑몰서버에서 지불취소에 대한 전자서명을 생성하여 결제서버에 전송하는 제6단계와,

상기 결제서버에서 상기 전자서명을 확인하여 정당한 전자서명인 경우에는 지불을 취소하고 취소확인에 대한 전자서명을 생성하여 상기 쇼핑몰서버에 전송하는 제7단계

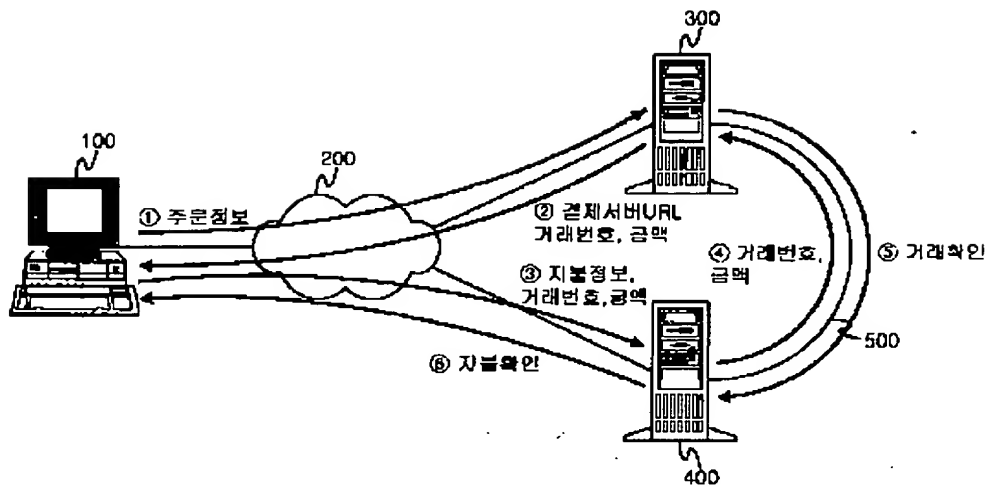
를 더 포함하는 것을 특징으로 하는 인터넷 상에서의 전자결제방법.

**도면**

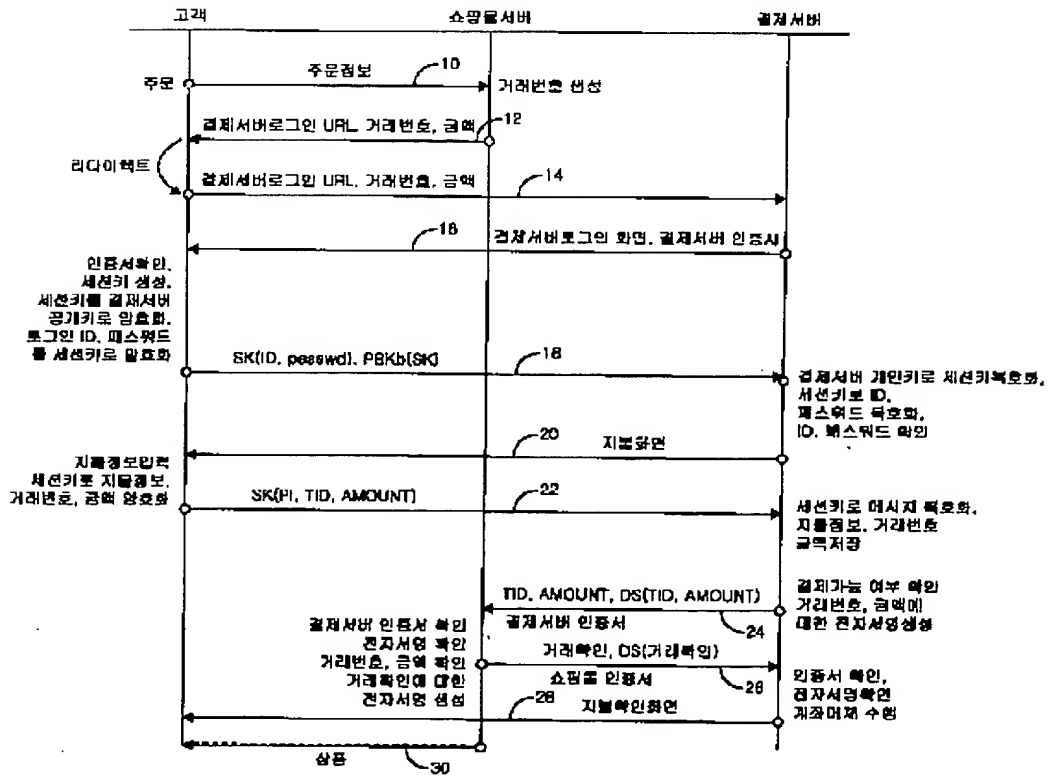
**도면 1**



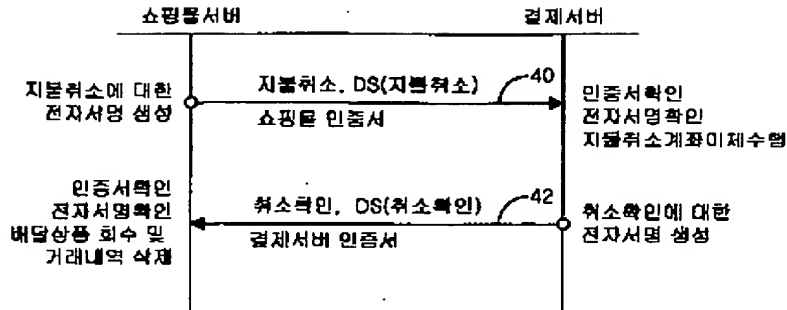
**도면 2**



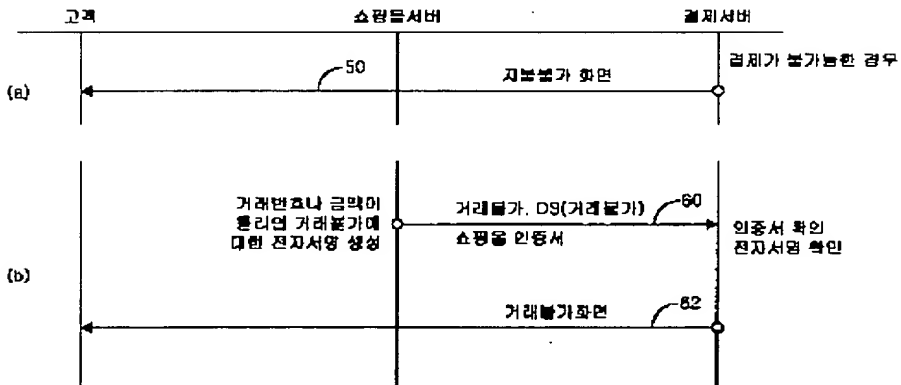
도면3



도면4



도면5



도면6

구입상품	SK휴대폰 IM-1100		
수량	1	가격	220,000
지불방법	현금전자지불 ▼		
확인		취소	

도면7

하기 금액을 당 은행의 계좌에서 지불하시겠습니까? 지불하시고자 하는 경우에는 계좌번호와 계좌의 비밀번호를 입력하시고 확인 버튼을 눌러 주십시오.

계좌번호	
비밀번호	
확인	취소